Résumé de cours sur les structures algébriques

I - Notion de groupe

I.1 - Généralités

Définition 1 (Notion de loi de composition interne) *Soit E un ensemble. On appelle loi de composition interne sur E une application $f : E \times E \to E$. Si x et y sont dans E, on note $x * y$ l'image de (x, y) par f. On dit aussi que l'ensemble E est stable par $*$.*

Exemple: Le produit vectoriel est une LCI sur l'ensemble des vecteurs de l'espace mais pas le produit scalaire.

Définition 2 (Notion de groupe) *Soit G un ensemble et $*$ une loi. On dit que $(G, *)$ est un groupe si :*

- *l'ensemble G est stable par $*$: $\forall x, y, \in G, x * y \in G$.*
- *la loi $*$ est associative : $\forall (x, y, z) \in G^3,\ (x * y) * z = x * (y * z)$.*
- *la loi $*$ admet un élément neutre : $\exists e \in G, \forall x \in G, x * e = e * x = x$.*
- *tout élément x de G admet un symétrique pour la loi $*$: $\exists a \in G,\ x * a = a * x = e$.*

Si la loi $*$ est commutative, on dit que le groupe G est commutatif.

Proposition 3 (Groupes de références) *Les ensembles suivants ont des structures de groupe*

- *pour la loi $+$: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$. L'élément neutre est 0.*
- *pour la loi $\times$: $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$. L'élément neutre est 1.*
- *pour la loi $\circ$: l'ensemble $(S_E, \circ)$ des bijections de E dans E est un groupe. L'élément neutre est l'application identité id_E.*
- *pour la loi $\times$: le groupe $(GL_n(\mathbb{K}), \times)$ des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$. L'élément neutre est la matrice unité I_n.*
- *Le groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ des classes de congruence modulo 4 (programme SPE).*

Remarque: L'ensemble $(\mathbb{N}, +)$ n'est pas un groupe car 2 n'admet pas de symétrique puisque $-2 \notin \mathbb{N}$. De même $(\mathbb{R}, \times)$ n'est pas un groupe, car 0 n'admet pas d'inverse.

Proposition 4 *Dans un groupe $(G, *)$, l'élément neutre e et les symétriques sont uniques.*

Remarque: On prendra garde aux notations, selon que la loi du groupe est notée «multiplicativement» $(*, \star, \circ)$ ou «additivement» $+$.

Définition 5 (Notations dans un groupe) *Soit $(G,*)$ un groupe d'élément neutre e (la loi est notée «multiplicativement»). Si $x \in G$, on note x^{-1} son symétrique, qu'on appelle l'inverse de x. Si n est un entier naturel, on pose*

$$x^0 = e \quad et \quad \forall n \in \mathbb{N}^*, x^n = x * x * \cdots * x.$$

On définit aussi x^n avec un exposant négatif : si $n \in \mathbb{N}^*$, on note x^{-n} l'inverse de x^n, c'est-à-dire $x^{-n} = (x^n)^{-1}$.

loi		*neutre*	*symétrique*	*n-ième itéré*	*cas où n négatif*
$*$	$x * y$	e	x^{-1} *inverse de* x	$x * x * \cdots * x = x^n$	$x^{-n} = (x^n)^{-1}$
$\times$	$x \times y$	1	x^{-1} *inverse de* x	$x \times x \times \cdots \times x = x^n$	$x^{-n} = (x^n)^{-1}$
$+$	$x + y$	0	$-x$ *opposé de* x	$x + x + \cdots + x = nx$	$(-n)x = -(nx)$

Proposition 6 (Règles de calcul) *Soit $(G,*)$ un groupe.*

- *Inverse d'un produit :*
$$\forall (x,y) \in G^2,\ (x*y)^{-1} = y^{-1} * x^{-1}.$$
- *Inverse d'un itéré :*
$$\forall n \in \mathbb{N}, \forall x \in G, (x^n)^{-1} = (x^{-1})^n.$$
- *Produit d'itérés :*
$$\forall n, m \in \mathbb{Z},\ \forall x \in G,\ x^n * x^m = x^{m+n}.$$
- *Simplification dans un groupe :*
$$\forall x, y, z \in G,\ x * z = y * z \implies x = y.$$

Remarque: Attention, en général si x et y sont dans $(G,*)$, on n'a pas $(x*y)^2 = x^2 * y^2$. Penser aux matrices...

I.2 - Sous-groupes

Définition 7 (Notion de sous-groupe) *Soit $(G,*)$ un groupe et H un ensemble. On dit que H un sous-groupe de $(G,*)$ si :*

- *H est une partie de G.*
- *H contient le neutre e de G*
- *H est stable pour la loi $*$ et par passage au symétrique,*
$$\forall (x,y) \in H^2,\ x * y \in H \quad et \quad x^{-1} \in H.$$

Remarque: La condition de stabilité $\forall (x,y) \in H^2,\ x*y \in H$ et $x^{-1} \in H$ est équivalent à $\forall (x,y) \in H^2,\ x * y^{-1} \in H$. Ainsi si la loi du groupe est notée $+$, la condition de stabilité s'écrit $x - y \in G$.

Proposition 8 *Si H est un sous-groupe de $(G,*)$, alors $(H,*)$ est un groupe.*

Remarque: Pour montrer qu'un ensemble est un groupe, on peut ainsi montrer que c'est un sous-groupe d'un groupe de référence.

Exemple:

- L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*,\times)$. Et $\{z\in\mathbb{C} \mid \text{Re}(z)=1\}$?
- L'ensemble $5\mathbb{Z}$ des multiples de 5 est un sous-groupe de $(\mathbb{Z},+)$.
- (Voir exos) Réciproquement tout sous-groupe H de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ (on pose $a=\min H\cap\mathbb{N}^*$ et si $x\in H$, on écrit $x=aq+r$, avec $0\leqslant r<a$. On a alors $r=x-aq\in H$, donc $r=0$).

Exercice 1 Soit G un sous-groupe de $(\mathbb{Z},+)$ qui contient les entiers 5 et 3. Que dire de G ?

I.3 - Notion de morphisme

On désire comparer des groupes. Pour cela nous allons introduire la notion de morphisme de groupe, puis d'isomorphisme.

Définition 9 *une application f du groupe $(G,*)$ vers le groupe $(H,\bullet)$ est un morphisme de groupe si*

$$\forall (x,y)\in G^2,\ f(x*y)=f(x)\bullet f(y).$$

Si de plus le morphisme f est bijectif, on dit que f est un isomorphisme de G sur H. Les groupes G et H sont dits alors isomorphes.

Exemple:

- L'application ln est un isomorphisme de $(\mathbb{R}^*,\times)$ vers $(\mathbb{R},+)$.
- L'application $\phi:(\mathbb{R},+)\to(\mathbb{C}^*,\times)$ défini par $\phi(t)=\mathrm{e}^{it}$ est un morphisme de groupe.
- Les groupes $(3\mathbb{Z},+)$ et $(\{5^n \mid n\in\mathbb{Z}\},\times)$ sont isomorphes.

Exercice 2 Soit $f:(]0,+\infty[,\times)\to(\mathbb{R},+)$ un morphisme de groupes. Déterminer $f(1)$, puis démontrer que $\forall x\in]0,+\infty[$ et $\forall r\in\mathbb{Q}, f(x^r)=rf(x)$.

Proposition 10 *Soit $f:(G,*)\to(H,\bullet)$ un morphisme de groupes. Alors f transforme l'élément neutre de G en élément neutre de H et transforme un symétrique dans G en symétrique dans H :*

$$f(e_G)=e_H \quad et \quad \forall x\in G,\ f(x^{-1})=(f(x))^{-1}.$$

Exercice 3 On pose $K=\{\text{diag}(\pm1,\pm1)\}$. Démontrer que K est un sous-groupe de $GL_2(\mathbb{R})$, qui n'est pas isomorphe au groupe $(\mathbb{U}_4,\times)$. On pourra regarder le carré des éléments des groupes.

Proposition 11 *Soit $f:(G,*)\to(H,\bullet)$ un morphisme de groupes.*

- *Si K est un sous-groupe de G, alors son image par f, noté $f(K)$ est un sous-groupe de H.*
- *Si L est un sous-groupe de H, alors son image réciproque par f, notée $f^{-1}(L)$ est un sous-groupe de G.*

Définition-Proposition 12 (Noyau et image d'un morphisme) *Soit $f : (G, *) \to (H, \bullet)$ un morphisme de groupes.*

- *On appelle noyau de f, l'ensemble noté $\mathrm{Ker}\, f$ défini par :*
$$\mathrm{Ker}\, f = \{x \in G \mid f(x) = e_H\}.$$
- *On appelle image de f, l'ensemble noté $\mathrm{Im}\, f$ défini par :*
$$\mathrm{Im}\, f = \{f(x) \mid x \in G\}$$

L'ensemble $\mathrm{Ker}\, f$ est un sous-groupe de G et l'ensemble $\mathrm{Im}\, f$ est un sous-groupe de H.

Exemple: le morphisme $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $f(t) = \mathrm{e}^{it}$. On a $\mathrm{Ker}\, f = 2\pi\mathbb{Z}$ et $\mathrm{Im}\, f = \mathbb{U}$.

L'ensemble $\mathrm{Ker}\, f$ est l'ensemble des antécédents du neutre e_H. Le résultat suivant est très utile pour prouver qu'un morphisme est injectif.

Proposition 13 *Soit $f : (G, *) \to (H, \bullet)$ un morphisme de groupes. On a*
$$f \text{ injective} \iff \mathrm{Ker}\, f = \{e_G\}.$$

Remarque: Le noyau mesure ainsi le défaut d'injectivité d'un morphisme.

II - Notion d'anneau

Définition 14 *Soit A un ensemble et $+$ et $\times$ deux lois. On dit que $(A, +, \times)$ est un anneau si :*

- *$(A, +)$ est un groupe commutatif.*
- *A est stable pour la loi $\times$*
- *La loi $\times$ est associative.*
- *la loi $\times$ admet un élément neutre noté 1_A ou 1 appelé unité de A.*
- *La loi $\times$ est distributive par rapport à $+$.*

Proposition 15 (Anneaux de référence) *Les ensembles suivants ont une structure d'anneau*

- $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{C}, +, \times)$

- $(\mathbb{K}[X], +, \times)$
- $(\mathcal{M}_n(\mathbb{K}), +, \times)$
- $\mathcal{F}(\mathbb{R}, \mathbb{R})$ *l'ensemble des fonctions de* $\mathbb{R}$ *dans* $\mathbb{R}$
- *les anneaux de congruence modulo n* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *(programme SPE)*

Remarque: les éléments de A ne sont pas forcément inversibles pour la loi $\times$.

Proposition 16 (Groupe des inversibles d'un anneau) *L'ensemble des éléments inversibles d'un anneau est un groupe pour la loi* $\times$.

Exemple:

- dans $\mathbb{Z}$, les seuls inversibles sont ± 1.
- dans $\mathbb{K}[X]$ les inversibles sont les polynômes constants non nuls
- dans $\mathcal{M}_n(\mathbb{K})$, les inversibles sont les matrices inversibles, c'est-à-dire $GL_n(\mathbb{K})$.
- dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{3}$ est inversible car $3 \times 3 = 9 \equiv 1 \mod 4$ donc $\overline{3} \times \overline{3} = \overline{1}$, mais $\overline{2}$ n'est pas inversible.

Proposition 17 (Règles de calcul) *Soit* $(A, +, \times)$ *un anneau. Soit* a *et* b *dans* A.

- $a \times 0_A = 0_A = 0_A$
- $a \times (-b) = (-a) \times b = -a \times b$
- *Formule du binôme de Newton : si* a *et* b *commutent* $(a \times b = b \times a)$,

$$\forall n \in \mathbb{N},\ (a+n)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k}.$$

Définition-Proposition 18 (Sous-anneau) *On dit qu'un ensemble* B *est un sous-anneau de l'anneau* $(A, +, \times)$ *si :*

- B *est inclus dans* A.
- B *contient le zéro* 0_A *et l'élément unité* 1_A *de* A
- B *est stable par différence et par produit (pour la loi* $\times$*) :*

$$\forall x, y \in B, x - y \in B \quad et \quad x \times y \in B$$

L'ensemble $(B, +, \times)$ *est alors un anneau.*

Exercice 4 On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss. Démontrer que $(\mathbb{Z}[i], +, \times)$ est un anneau, puis déterminer ses éléments inversibles.

Remarque: L'anneau des entiers de Gauss est par exemple utile pour prouver le théorème des deux carrés. Tout comme $\mathbb{Z}$ et $\mathbb{K}[X]$, il dispose d'une division euclidienne, on parle d'anneau euclidien. Une égalité comme $5 = (1-2i)(1+2i)$ montre alors que 5 n'est pas un nombre premier dans $\mathbb{Z}[i]$.

Définition 19 (Anneau intègre) *Un anneau A est intègre s'il vérifie la propriété suivante :*

$$\forall (x,y) \in A^2,\ (x \times y = 0 \Rightarrow (x = 0 \quad ou \quad y = 0))\,.$$

Remarquons qu'il s'agit de la fameuse propriété apprise au collège : si un produit est nul alors l'un des facteurs est nul.

Exemple:

- L'anneau $\mathbb{K}[X]$ est intègre
- L'anneau $\mathcal{M}_n(\mathbb{K})$ n'est pas intègre puisqu'il existe des matrices nilpotentes non nulles.
- $\mathcal{F}(\mathbb{R},\mathbb{R})$ pas intègre
- $\mathbb{Z}/4\mathbb{Z}$ non intègre car $\overline{2} \times \overline{2} = \overline{0}$

Remarque : si on peut définir la notion de morphisme d'anneau.

III - Notion de corps

Définition 20 (Corps) *Un corps est un anneau (commutatif) dans lequel tout élément non nul est inversible.*

Proposition 21 (Corps de référence) *Les ensemble suivants sont des corps :*

$$(\mathbb{Q},+,\times),\ (\mathbb{R},+,\times),\ (\mathbb{C},+,\times).$$

Remarque:

1. Culture : ll existe des corps non commutatifs, par exemple le corps des quaternions.
2. L'année prochaine, vous verrez que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement, si n est un nombre premier.

Proposition 22 *Tout corps est un anneau intègre.*